Conjunctive Keyword Search with Key Wrapping and Sponge Re Encryption Function for E-Health Clouds

YELUDUTI RAVI[#1] **, RATNAKUMAR JALA**[#2]

[#1] M.Tech Scholar,Department of Computer Science and Technology,
Baba Institute of Technology and Sciences,Visakhapatnam,AP,India.

[#2] HOD & Associate Professor,Department of CSE,
Baba Institute of Technology and Sciences,Visakhapatnam,AP,India.

ABSTRACT

As we all know that electronic health (e-health) record system becomes a novel application that will bring great convenience especially in the healthcare domain. This mainly came into existence in order to give security for the sensitive information of the patients who want to retrieve the information from the concern hospitals. Now a days the distributed healthcare systems under the roof of cloud computing server is used as a main facility for extracting the patient information among various health care service providers. This proposed thesis mainly concentrate on two things like one for data confidentiality and other one is to keep the patients identity very secure. Till now there are various primitive methods to control the access and provide the anonymous authentication, but they were not exploited according to the user need. In order to resolve all the above issues, in this proposed application we try to design and analyze the novel authorized privacy accessible model (APAM) for providing high level of security for the patient's information which is accessed over online. By using this proposed model, the patients can authorize physicians by setting an access tree which takes the threshold value as input, then, based on the threshold value what we take, we try to design and analyze a new attribute based designated method for verifying the identity or signature of the patient whose data is stored in the cloud. By conducting various experiments on our proposed PSMPA model by taking some sample patient information files into the cloud, our simulation results clearly tell that our proposed model is best suited of providing security for the sensitive information, which is shared among multiple organizations.

KEYWORDS

Health Care Information, Distributed Service Providers, Keyword Search, Anonymous Authentication, Designated Verifier Signature.

1. INTRODUCTION

As we all know that cloud server has attained a lot of people attention in storing their valuable and important data inside the server. It still faces a lot of limitations in terms of data accessing and storage especially with a sensitive data. In recent days a lot of medical companies try to insert their valuable patients information inside the cloud storage and try to access the same data from the cloud server whenever they need. But this leads to a major problem like un-authorized data access in odd times [1], [2].Actually all the data which is uploaded into the cloud server is mainly accessed by various users who are interrelated to that cloud. The users who got an access with that current cloud can connect to the cloud server and in turn access the data from the cloud server.In this proposed thesis we mainly use the DRIVEHQ as the live cloud storage server for accessing the files to and from the local server to real time cloud.

From the below figure 1, we can observe a variety of cloud service providers that are available in the real world for integrating with the software companies for storing and accessing the data remotely to and from the server.One among the best is DRIVEHQ and BOX.com as both the clouds are almost hybrid in nature because they can provide storage in public manner as well as in private manner.So the user who just registered with free of use can get public access with a space of 1 GB and the same user who wish to store the large amount of data despite of the size of data then he need to pay the amount for becoming the premium user,then such a cloud account will become as private cloud.If the same user want free as well as paid storage at a time,then such an account is known as private cloud data storage.

As we all know that there were a lot of data users who try to share a lot of information in online through various OSN sites, such as Face book, MySpace, and Twitter.

FIGURE.1.SHOWS THE LIST OF SEVERAL REAL TIME CLOUD SERVICE PROVIDERS

They have no security in sharing the information with one another. At that point of view a lot of companies who want to share their valuable information in a secure manner, proposed a new form of data sharing and data accessing known as cloud computing [3]–[5] in a centralized manner. This mechanism is treated as one of the most promising approach to solve the explosive expanding of data sharing. In cloud computing, to protect data from leaking, users need to encrypt their data before being shared. As we all know that cloud data can be easily shared and accessed among all the members inside the cloud,Access control [6], [7] plays a vital role or it is a paramount for the first line of defense that prevents unauthorized access to the shared data. Recently, attribute-based encryption (ABE) [8]–[10] has been attracted much more attentions since it can keep data privacy and realize fine-grained, one-to-many, and non interactive access control. CP-ABE scheme [11]–[13] is one of feasible schemes which has much more flexibility and is more suitable for general applications.

2. BACKGROUND WORK

In this section we mainly discuss about the various assumptions that are used in the proposed paper for Conjunctive Keyword Search with Key Wrapping and Sponge Re Encryption Function for E-Health Clouds. Now let us discuss about those things in detail as follows:

A) Main Motivation

The main motivation for designing this application is to provide security for the data which is stored inside the cloud server rather than storing the same data in the individual local server.Here we mainly discuss about the differences between a local server and a dedicated cloud server storage.Actually if we compare the both storage in many aspects the cloud servers also work in the same wat like the normal physical servers but only the difference is normal servers can be hosted with in our limits and they can be access with the boundary limits.But for the live or cloud server we can access the file remotely and we can access all the data in all the times despite of time or area.

In the traditional data storage or data hosting,they are two types of hosting Models that are done in real time environment. They are as follows:

1. Shared Hosting Model (&)
2. Dedicated Hosting Model.

B) CLOUD STORAGE TYPES

As in our proposed application, we are using the cloud server account for storing the patient information very securely in the cloud server and try to access the same at the time of user need. We try to observe about some of the types of cloud data storage that are available in the real world environment. Now let us look about those in detail as follows:

i) PERSONAL STORAGE

This is a well known storage which we regularly use with the help of our personal computers or mobiles or palmtops. Here the data can be accessed from anywhere at any time despite of the location or region.It is mainly used for data synchronizing and data sharing in a open access manner. The best example for personal storage of cloud is Apple cloud which can be run through a iphone at any time.

ii) PUBLIC STORAGE

Public cloud storage is where the enterprise and storage service provider are separate and there aren't any cloud resources stored in the enterprise's data center. The cloud storage provider fully manages the enterprise's public cloud storage. Normally in the current days all the cloud storage providers provide public cloud as storage medium with min 2GB and Max 10 GB for data storage with free data access and usage. If that space exceeds then we need to pay the excess storage cost more than 10 GB, which acts as a private cloud.

iii) PRIVATE CLOUD STORAGE

It is a form of cloud storage where the enterprise and cloud storage provider are integrated in the enterprise's data center. In private cloud storage, the storage provider has infrastructure in the enterprise's data center that is typically managed by the storage provider. Private cloud storage helps resolve the potential for security and performance concerns while still offering the advantages of cloud storage.

iv) HYBRID CLOUD STORAGE

Hybrid cloud storage is a combination of public and private cloud storage where some critical data resides in the enterprise's private cloud while other data is stored and accessible from a public cloud storage provider. A Hybrid Cloud Storage is the combination of public and private cloud storage, till less than 10 GB it is treated as public cloud and more than 10 GB treats as a private cloud storage. Hence an account which contains both these combine is known as hybrid cloud data storage.

3. PROPOSED NOVEL AUTHORIZED PRIVACY ACCESSIBLE (APAM) MODEL

In this proposed application we try to use the novel authorized privacy accessible model for providing security for the patients related information to be stored in the cloud server with timing enabled .Now let us discuss about that in detail as follows:

In the below Figure. 2,we can clearly show the working flow of our proposed model for the electronic health reports storage.We can see mainly 3 different roles that are available in the below architecture

1. Owner,
2. User/Client &
3. Data Storage Center.

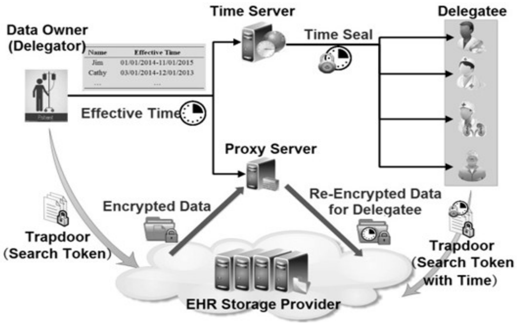

Figure.2. Represents the Architecture of Proposed Novel Authorized Privacy Accessible (APAM) Model

Initially the data owner tries to store his private EHR files on a third-party database. He extracts keywords from the EHR files and encrypts those plaintext keywords into the secure searchable indices. The EHR files are encrypted to ciphertext. Then, that information is outsourced to the datacenter.

Now the data center consists of an EHR storage provider and a search server. The storage provider is responsible for storing data and search server performs search/add/delete operations according to users' requests. A user generates a trapdoor to search the EHR files using his private key and sends it to the search servers. After receiving the request, the search servers interact with the EHR storage provider to find the matched files and returns those retrieved information to the user in an encrypted form.

From the above figure 2, the timing enabled proxy re-encryption technique can also be shown searchable encryption model is shown. In this model, we mainly try to show the importance of the time enabled function as this is a very new primitive that was still not yet implemented in EHR.we highlight the implementation of the time controlled function. The data owner who wants to upload a file into the cloud server will initially try to upload the files into the cloud server with a basic privilege of 1 day access.I.e 24 hours as default access time for all the files. If any data user or patient who want to access the file after the stipulated date and time, then the data owner should send a request for the proxy server to enable the timer for the expired files[14].

As the proxy server will receive the information from the data owner in this manner like "RAVI, 01/10/2017 – 06/10/2017". It indicates that the delegate RAVI is authorized and approved to access the files from the start date and end date which is specified by the data owner.The proxy server once after receiving the queries from the data owner, it will immediately update the same to the time server for extending the timer for the expired files.

The time seal is a trapdoor of an effective time period and concealed by the private key of the time server.In the re-encryption operation, the proxy server will encapsulate the effective time into the re-encrypted ciphertext. In order to reduce computing cost, the proxy server will not re-encrypt the ciphertext until they are accessed, which is so called lazy re-encryption mechanism [15]. In the query phase, the data owner can conduct ordinary search operations with his own private key. However, the delegatee has to generate a keywords trapdoor with the help of the time seal. The cloud data server will not return the matched files unless the effective time encapsulated in the time seal accords with the time in the re-encrypted ciphertext, which is different from traditional proxy re-encryption SE schemes.

4. IMPLEMENTATION MODULES

Implementation is the stage where theoretical design is converted into practical design. Here we divide the application into various modules and then decide the flow of the application in a modular fashion. The following are the 5 modules for this application.

1) Delegator owner Module
2) Delegate Module
3) Conjunctive keywords search
4) Proxy re-encryption
5) Time controlled revocation

Now let us discuss about these modules in short as follows:

1. Delegator Owner Module

The authority delegation is realized mainly by proxy re-encryption mechanism. The proxy server makes use of the re-encryption key to transform the cipher text encrypted by delegator's public key into another form, which can be searched by the delegate using his own private key.

2. Delegate Module

The delegatee will be divested of the search authority when the effective time expires. In order to achieve the time controlled access right revocation, the predefined time information is embedded in the re-encrypted cipher text with a time seal. With the help of the time seal, the delegate is able to generate a valid delegation trapdoor by *Trapdoor* algorithm. If the time information hidden in the re-encrypted ciphertext is inconsistent with that in the delegation trapdoor, the equation in *TestR* algorithm will not hold. Moreover, Workflow of proposed algorithm. the search query of the delegate will be rejected by the data server if the current time beyond the preset time.

3. Conjunctive Keywords Search

Compared with the single keyword search, the conjunctive keyword search function provides the users more convenience to return the accurate results that fulfills users' multiple requirements. The users do not have to query an individual keyword and rely on an intersection calculation to obtain what they needs. To the best of our knowledge, there is no existing proxy re-encryption searchable encryption scheme could provide the conjunctive keywords search capability without requiring a random oracle. Our scheme has solved this open problem. The scheme could provide both the conjunctive keywords search and the delegation function. Unfortunately, it is proved in the random oracle (R.O.) model, which greatly impairs the security level.

4. Proxy Re-Encryption

The proxy re-encryption technology is practical in EHR systems. It will greatly facilitate patient delegating the search and access rights. Schemes in could not provide the proxy re-encryption searchable encryption function to the users.

5. Time Controlled Revocation:

An important design goal is to enable time controlled access right revocation. The delegation appointment will terminate when the preset effective time period disagrees with the current time. It should prevent the authorized user from accessing the records overtime.

5. CONCLUSION

In this paper, we for the first time have proposed a novel authorized accessible privacy model and a patient self-controllable multi-level privacy preserving cooperative authentication scheme realizing three different levels of security and privacy requirement in the distributed healthcare data KeyWord cloud computing system are proposed, followed by the formal security proof and efficiency evaluations which illustrate our PSMPA can resist various kinds of malicious attacks and far outperforms previous schemes in terms of storage, computational and communication overhead.

6. REFERENCES

[1] L. Fang, W. Susilo, C. Ge, and J. Wang, Public key encryption with keyword search secure against keyword guessing attacks without random oracle, *Inf. Sci.*, vol. 238, pp. 221–241, Jul. 2013.

[2] M.-S. Hwang, S.-T. Hsu, and C.-C. Lee, A new public key encryption with conjunctive field keyword search scheme, *Inf. Technol. Control*,vol. 43, no. 3, pp. 277–288, 2014.

[3] D. Boneh and B. Waters, Conjunctive, subset, and range queries.

[4] S. Quinlan and S. Dorward. Venti: a new approach to archival storage. In *Proc. USENIX FAST*, Jan 2002.

[5] J. Xu, E.-C. Chang, and J. Zhou. Weak leakage-resilient client-side deduplication of encrypted data in cloud storage. In *ASIACCS*, pages 195–206, 2013.

[6] K. Liang, J. K. Liu, D. S. Wong, and W. Susilo, An efficient cloud based revocable in *Proc. 19th*.

[7] T. H. Yuen, Y. Zhang, S. M. Yiu, and J. K. Liu, Identity-based encryption with post-challenge auxiliary inputs for secure cloud applications and sensor networks, in *Proc. 19th Eur. Symp. Res.*

[8] K. Liang *et al.*, A DFA-based functional proxy re-encryption scheme for secure public cloud data sharing, *IEEE Trans. Inf. Forensics Security*,vol. 9, no. 10.

[9] T. H. Yuen, J. K. Liu, M. H. Au, X. Huang, W. Susilo, and J. Zhou, "*k*-times attribute-based anonymous access control for cloud computing,"*IEEE Trans. Comput.*, vol. 64, no. 9, pp. 2595–2608, Sep. 2015.

[10] J. K. Liu, M. H. Au, X. Huang, R. Lu, and J. Li, Fine-grained two factor access control for Web-based cloud computing services.

[11] A. Sahai and B. Waters, Fuzzy identity-based encryption, in *Advances in Cryptology*. Berlin, Germany: Springer, May 2005, pp. 457–473.

[12] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in *Proc. 13th ACM Conf. Comput. Commun. Secur.*, Oct. 2006, pp. 89–98.

[13] W. Zhu, J. Yu, T. Wang, P. Zhang, and W. Xie, "Efficient attribute-based encryption from R-LWE," *Chin. J. Electron.*, vol. 23, no. 4, pp. 778–782,Oct. 2014.

[14] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute based encryption," in *Proc. IEEE Symp. Secur. Privacy*, May 2007,pp. 321–334.

[15] L. Cheung and C. Newport, "Provably secure ciphertext policy ABE," in *Proc. 14th ACM Conf. Comput. Commun. Secur.*, Oct. 2007,pp. 456–465.

7. ABOUT THE AUTHORS

YELUDUTI RAVI is currently pursuing her 2 years M.Tech in Department of Computer Science and Technology at Baba Institute of Technology and Sciences, Visakhapatnam, AP, India. Her area of interest includes Cloud Computing.

RATNAKUMAR JALA is currently working as an HOD & Associate Professor in Department of Computer Science and Engineering at Baba Institute of Technology and Sciences, Visakhapatnam, AP, India.He has more than 12 years of teaching experience in various engineering colleges. He published more than 5 scopus indexed journals in various international journals. His research interest includes Software Engineering.